

LOGIC CIRCUIT WITH VARIABLE INTERNAL POLARITIES

Related Application

The present application is a continuation of International Application No. PCT/FR01/04069 filed on December 19, 2001, the entire disclosure of which is
5 incorporated herein by reference.

Field of the Invention

The present invention relates to secured integrated circuits and a method for scrambling the operation of logic circuits in these integrated
10 circuits. The present invention particularly relates to integrated circuits in smart cards, electronic labels, electronic badges, and in secured portable electronic objects.

Background of the Invention

15 Electronic transactions carried out by smart card are secured by using a smart card authentication procedure that uses an encryption algorithm. During the authentication procedure, the terminal used for the transaction sends the smart card a random code. The
20 smart card must respond to the terminal by producing an authentication code which is the transform of the random code by the encryption algorithm. The terminal calculates the transform of the random code and

compares the result obtained with the one returned by the card. If the authentication code returned by the card is valid, the transaction is authorized.

In the integrated circuit of a smart card,
5 the encryption algorithm is generally performed by a hard-wired logic circuit, or encryption co-processor, to which a secret key is assigned that is stored in a protected area of the integrated circuit memory. It is essential to guarantee absolute protection of the
10 secret key as the encryption algorithms implemented in the authentication procedures are known, and only the secret key guarantees the tamper resistance of the authentication procedure.

However, in recent years, pirating techniques
15 of integrated circuits have progressed considerably and criminals now have sophisticated analysis methods that enable them to detect the secret keys of the encryption algorithms by monitoring certain logic and/or electric signals that are part of the integrated circuit
20 operation. Some of these methods are based on monitoring the current consumed by an integrated circuit during the execution of confidential operations.

In particular, SPA type (single power
25 analysis) methods and DPA type (differential power analysis) methods can be singled out, the latter being particularly dangerous as they allow a secret key to be discovered without the need to monitor the data circulating on the integrated circuit data bus.

30 Other pirating methods use electrical probes (so-called probing methods) and are based on monitoring logic signals occurring in the logic circuits, particularly in the encryption circuits. For this

purpose, small orifices are made in the integrated circuit board to access the logic circuit nodes. These orifices are then filled with a conductive material to form contact areas on the surface of the integrated circuit from which the polarity of the logic signals can be monitored.

To counter these pirating methods, there are various counter-measures that include, for example, using a random clock signal, using dummy codes, masking the variations in the current consumption of logic circuits by current generators, scrambling the current consumption of these circuits by the use of noise generators, etc.

However, it is well known that each new anti-pirating method devised generally ends up being countered by the criminals, who have powerful calculation and analysis means. Generally speaking, various anti-pirating methods may be combined to provide more efficient protection.

Summary of the Invention

In view of the foregoing background, an object of the present invention is to provide a method for scrambling the operation of an integrated circuit, particularly a logic circuit performing an encryption algorithm. This method is intended as an additional means of combating piracy, and is intended to be combined, if necessary, with other known anti-pirating methods to improve the security of secured integrated circuits.

This and other objects, advantages and features of the present invention are provided by a logic circuit that performs a logic function with N

data inputs and M data outputs, with N being at least equal to 2 and M being at least equal to 1. The logic circuit comprises logic gates and/or transistors to perform the logic function in at least two different
5 ways. The way in which the logic function is performed is determined by the value of a function selection signal applied to the logic circuit.

Thus, for identical data applied at the input of the logic circuit and different function selection
10 signal values, the polarities of certain internal nodes of the logic circuit and/or the current consumption of the logic circuit are not identical.

According to one embodiment, the logic circuit comprises a logic block having N inputs linked
15 to the data inputs of the logic circuit and M outputs linked to the data outputs of the logic circuit. The logic block performs a first logic function or a second logic function according to the value of the function selection signal, and includes a circuit or means for
20 reversing the data applied to the logic block and for reversing the data delivered by the logic block when the selection signal has a determined value. The means for reversing the data applied may comprise EXCLUSIVE-OR gates that receive the function selection signal at
25 one input.

According to another embodiment, the logic circuit comprises logic gates performing a NAND
function when the function selection signal has a first logic value and a NOR function when the function
30 selection signal has a second logic value. The logic circuit may be linked to a random signal generator that delivers a random function selection signal. The logic function may also be an encryption function.

The present invention also relates to an encryption circuit comprising a plurality of encryption blocks each comprising a logic circuit according to the present invention.

5 According to one embodiment, the encryption circuit is linked to a random signal generator for applying a random function selection signal to each encryption block, the value of which is independent of the function selection signal applied to the other
10 encryption blocks.

The present invention also relates to a secured integrated circuit comprising a plurality of logic circuits as described above, and means or a circuit for applying a random-type function selection
15 signal to the logic circuits. The value of the function selection signal is modified at random at least after each integrated circuit reset.

The integrated circuit may comprise a microprocessor or a central processing unit (CPU). The
20 integrated circuit may also be arranged on a portable support to form a smart card or any other equivalent portable electronic object.

The present invention also relates to a logic gate comprising N data inputs and one output. A first
25 group of transistors is arranged to perform a first logic function, a second group of transistors is arranged to perform a second logic function, and function selection means are arranged to receive a function selection signal. The function selection
30 means validates one of the two logic functions at the logic gate output according to the function selection signal value.

According to one embodiment, the function selection means comprise transistors arranged to short-circuit transistors assigned to perform one of the two functions, according to the function selection signal value. The function selection means may also comprise transistors to interrupt conductive paths of the transistors assigned to perform one of the two functions, according to the selection signal value. The logic gate may comprise two inputs. The first logic function may be the NAND function and the second logic function may be the NOR function.

The present invention also relates to a logic circuit comprising a plurality of logic gates as described above. The logic circuit has one input to receive a function selection signal applied to the logic gates.

Another aspect of the present invention relates to a method for scrambling the operation of a logic circuit provided to perform a logic function with N data inputs and M data outputs, with N being at least equal to 2 and M being at least equal to 1. The method preferably comprises a step of providing, in the logic circuit, logic gates and/or transistors arranged to perform the logic function in at least two different ways. The way in which the logic function is performed is determined by the value of a function selection signal applied to the logic circuit. The method may further include a step of applying a random function selection signal to the logic circuit, and a step of refreshing the function selection signal at determined instants so as to scramble the operation of the logic circuit.

According to one embodiment, the method comprises steps of providing, in the logic circuit, a logic block comprising N inputs linked to the data inputs of the logic circuit and M outputs linked to the data outputs of the logic circuit. The logic block performs a first logic function or a second logic function according to the function selection signal value. Logic gates reverse the data applied to the logic block and reverse the data delivered by the logic block when the selection signal has a determined value.

According to another embodiment, the logic block is achieved by logic gates performing the NAND function when the function selection signal has a first logic value, and the NOR function when the function selection signal has a second logic value.

Brief Description of the Drawings

These and other objects, advantages and features of the present invention shall be presented in greater detail in the following description of the method according to the present invention and of various examples of variable polarity logic circuits according to the present invention, in relation, but not limited to the following figures:

Figure 1 is a schematic representation of a variable polarity logic gate according to the present invention;

Figure 2 is an electrical diagram showing one embodiment of the logic gate illustrated in Figure 1;

Figure 3 represents, in block form, a variable polarity logic circuit according to the present invention;

Figure 4 represents, in block form, an example of a variable polarity logic circuit according to the present invention;

Figures 5A and 5B represent two logic functions performed by the variable polarity circuit illustrated in Figure 4 according to a value of the function selection signal applied to the logic circuit;

Figures 6A and 6B are timing diagrams representing logic signals occurring on the nodes of the logic circuit illustrated in Figure 4 for two function selection signal values;

Figure 7 represents, in block form, an example of embodiment of a variable polarity encryption circuit according to the present invention; and

Figure 8 represents, in block form, an example of a secured integrated circuit architecture comprising variable polarity logic circuits according to the present invention.

Detailed Description of the Preferred Embodiments

The present invention is based on the fact, as known by those skilled in the art, that any logic function can be performed using NAND type or NOR type elementary logic gates. Another fact on which the present invention is based is that a logic circuit architecture achieved by NAND gates and an identical logic circuit architecture in which the NAND gates are replaced by NOR gates, respectively perform two logic functions F1 and F2 which have certain similarities. More particularly, the result of the transformation of data A, B, C... by the function F1 is the opposite of

the result of the transformation of reversed data /A, /B, /C... by the function F2, which can be written as:

$$(1) F1(A, B, C...) = /[F2(/A, /B, /C...)]$$

On the basis of this relation, the present invention suggests achieving logic circuits capable of performing a logic function in two different ways, one using NAND gates and the other using NOR gates.

Before describing examples of embodiments of these logic circuits, a logic gate with two operating modes shall be described in relation to Figures 1 and 2 that can be used to achieve these logic circuits. In particular, this logic gate may form the basic cell of a computer-aided logic circuit design system.

Gate 10 shown in Figure 1 has two data inputs IN1, IN2, an auxiliary input AUX and one data output OUT, and comprises a NAND gate 1 and a NOR gate 2, each with two inputs. Inputs IN1, IN2 are linked to the corresponding inputs of gates 1 and 2 by two switches SW1, SW2 controlled by a function selection signal R applied at the input AUX. The outputs of gates 1 and 2 are linked to the output OUT by a third switch SW3, also controlled by the signal R.

When the signal R is on 0, inputs IN1, IN2 are connected to the inputs of gate 1 and the output of gate 1 is connected to the output OUT. When the signal R is on 1, inputs IN1, IN2 are connected to the inputs of gate 2 and the output of gate 2 is connected to the output OUT. Therefore, assuming that gate 10 receives bits A and B at the input, gate 10 performs the NAND function when R is equal to 0 and the NOR function when R is equal to 1. In other terms:

$$(2) \quad \text{OUT}_{(R=0)} = /(A*B) = \text{NAND}(A,B)$$

$$(3) \quad \text{OUT}_{(R=1)} = /(A+B) = \text{NOR}(A,B)$$

In addition, it can be noted that:

$$(4) \quad /[\text{NOR} (/A, /B)] = /[/ (/A + /B)] = /[A*B] = \text{NAND}(A,B)$$

5 Thus, the opposite of the transform of reversed data $/A$ and $/B$ by the NOR function is equal to the transform of non-reversed data A and B by the NAND function, which forms a special case of the general relation (1) mentioned above.

10 Figure 2 represents an example embodiment of logic gate 10 using NMOS and PMOS transistors. Gate 10 comprises a pull-up stage SPU polarized by a supply voltage V_{cc} and a pull-down stage SPD connected to ground (GND). The connection point of the two stages
15 form the node of output OUT of gate 10. The stage SPU is achieved using PMOS transistors and comprises a stage NOR1 in series with a stage NAND1. The stage SPD is achieved using NMOS transistors and comprises a stage NOR2 in parallel with a stage NAND2.

20 The stage NOR1 comprises two transistors TP1, TP2 in series and one transistor TP3 in parallel with these two transistors TP1, TP2. The sources of transistors TP1 and TP3 receive the voltage V_{cc} . The stage NAND1, arranged between stage NOR1 and the node
25 of output OUT, comprises three transistors TP4, TP5, TP6 in parallel. The stage NOR2 comprises two transistors TN1, TN2 in parallel, arranged in series with a transistor TN3. The source of transistor TN3 is connected to ground. The stage NAND2 comprises three

transistors TN4, TN5, TN6 in series. The source of transistor TN6 is connected to ground.

Gate 10 also comprises an inverting gate INV1 (achieved using a PMOS transistor and an NMOS transistor, not shown). The input of the inverting gate INV1 is connected to the input AUX, and the output delivers a signal \overline{R} . The input IN1 of gate 10, receiving bit A, is connected to the gates of transistors TP1, TP4, TN1, TN4. The input IN2, receiving bit B, is connected to the gates of transistors TP2, TP5, TN2, TN5. The input AUX receiving the signal R is connected to the gates of transistors TP3 and TN3. The output of gate INV1 delivering the reversed signal \overline{R} is connected to the gates of transistors TP6, TN6.

When the signal R is equal to 1 and \overline{R} is equal to 0, transistors TP3 and TN6 are blocked and transistors TP6 and TN3 are in a transmission state. The stage NAND1 is short-circuited by transistor TP6 and the stage NAND2 is inhibited. Transistor TN6, which links the stage NAND2 to ground, is blocked. The stages NOR1 and NOR2 are active and gate 10 operates like a NOR gate. Inversely, when R is equal to 0 and \overline{R} is equal to 1, the stage NOR1 is short-circuited (TP3 in transmission state) and the stage NOR2 is inhibited (TN3 blocked). The stages NAND1 and NAND2 are active and gate 10 operates like a NAND gate.

It will now be assumed, with reference to Figure 3, that a logic circuit 15 is to be achieved with two inputs IN1, IN2 and one output OUT, for performing a determined logic function F1. It will also be assumed that the F1 function can be achieved by a special arrangement of NAND logic gates.

According to a first aspect of the method of the present invention, the arrangement of NAND gates is maintained but the NAND gates are replaced by gates 10 according to the present invention to form a logic
5 block 11 that has two data inputs IN1', IN2', one data output OUT' and one input AUX. At the input AUX the logic block 11 receives the function selection signal R applied to the logic gates 10 that form it (not shown). This logic block 11 thus performs the function F1 when
10 R is equal to 0 and performs a function F2 when R is equal to 1. Gates 10 then operate as NOR gates. The function F2 is linked to the function F1 by the relation (1) mentioned above.

According to a second aspect of the method of
15 the present invention, three gates 12, 13, 14 of the EXCLUSIVE-OR type are then associated to the logic block 11 to form the complete logic circuit 15. Each gate 12, 13, 14 receives the function selection signal R at a first input. The second input of gate 12 is
20 connected to input IN1 of logic circuit 15, the second input of gate 13 is connected to input IN2 of logic circuit 15, and the second input of gate 14 is connected to the output OUT' of logic block 11. The output of gate 12 is connected to input IN1' of logic
25 block 11, the output of gate 13 is connected to input IN2' of logic block 11, and the output of gate 14 forms the output OUT of logic circuit 15.

By referring to the data applied to inputs IN1 and IN2 of circuit 15 as A and B, and the data
30 applied to inputs IN1', IN2' of block 11 as A' and B', the operation of logic circuit 15 is defined by the following relations:

when $R=0$:

$$A' = A, B' = B, OUT = OUT'$$

$$(5) \quad OUT_{(R=0)} = F1(A, B)$$

when $R=1$:

5 $A' = \neg A, B' = \neg B, OUT = \neg OUT'$

$$(6) \quad OUT_{(R=1)} = \neg F2(A', B') = \neg F2(\neg A, \neg B)$$

as the EXCLUSIVE-OR gates operate, in relation to data A, B and to the output OUT', as inverting gates when R is equal to 1 and as non-inverting gates when R is
10 equal to 0.

By combining relation (6) with the general relation (1), it results that:

$$(7) \quad OUT_{(R=1)} = \neg F2(\neg A, \neg B) = F1(A, B) = OUT_{(R=0)}$$

Thus, as seen from its inputs and its output,
15 logic circuit 15 always performs the same function F1, but in a different way when $R=0$ and when $R=1$. The result is that the polarities that the internal nodes of logic circuit 15 differ according to the value of R for identical data A, B applied at the input.

20 Therefore, as it will become clear, assigning a random value to the function selection signal R allows the polarities of the internal signals of logic circuit 15 to be modified at random without modifying the result it delivers, and thus allows its operation and current
25 consumption to be scrambled.

Figure 4 represents an example embodiment of a logic circuit 30 according to the present invention, with the straightforward case, chosen as an example, in

which the function F1 is the NAND function with four inputs. Circuit 30 thus has four inputs IN1 to IN4 receiving bits A, B, C, D and one output OUT delivering the result. In accordance with the architecture
5 proposed above, circuit 30 comprises a logic block 20 with four inputs IN1' to IN4' and one output OUT', along with EXCLUSIVE-OR gates 21 to 24 arranged between inputs IN1 to IN4 and inputs IN1' to IN4', and an EXCLUSIVE-OR gate 25 arranged between output OUT' and
10 output OUT.

Each gate 21 to 25 receives the function selection signal R at an input that is delivered by a random signal generator RGEN. Gates 21 to 24 receive one of bits A, B, C, D at their second input and
15 respectively deliver a bit A', B', C', D' to inputs IN1' to IN4'. Gate 25 receives the output OUT' of block 20 on its second input, and its output forms the output OUT of logic circuit 30. Logic block 20 comprises three cascade-arranged gates 10, 10', 10''
20 according to the present invention that replace conventional NAND gates. Each gate is monitored by the selection signal R. Gate 10 therefore receives bits A and B at an input, gate 10' receives bit C' at an input and a signal X1 delivered by gate 10, and gate 10''
25 receives bit D' at an input and a signal X2 delivered by gate 10'.

In Figure 5A, block 20 is equivalent to three cascade-connected NAND gates when R is equal to 0. In Figure 5B, block 20 is equivalent to three cascade-
30 connected NOR gates when R is equal to 1. In accordance with relation (7), the function performed by logic circuit 30 seen from its inputs and its output is the NAND function, regardless of the value of signal R

due to the EXCLUSIVE-OR gates that reverse the inputs and the output of circuit 30 when R is equal to 1.

Figure 6A shows the operation of circuit 30 when bits A to D applied to inputs IN1 to IN4 have a sequence of determined values, and when R is equal to 0. Figure 6B shows the operation of circuit 30 when the same sequence of bits is applied to circuit 30 and when R is equal to 1. Each of these figures features the timing diagrams of signals A', B', C', D', X1, X2, OUT' and OUT. These figures clearly show that the polarities of these various signals are reversed when R is equal to 1, although the sequence delivered by the output OUT does not change. Therefore, for example, signal X1 goes to 0 at an instant t1 when R is equal to 0 and goes to 1 at the same instant t1 when R is equal to 1.

As the value of the function selection signal R is preferably random, the logic values occurring on the nodes of this logic circuit have a non-predictive and non-repetitive character. This property of a logic circuit according to the present invention combats the pirating techniques mentioned above, particularly pirating by monitoring logic signals (i.e., probing) or by monitoring the current consumption of the logic circuit (i.e., a DPA-type attack). In fact, as the instantaneous consumption of the logic circuit is a function of the number of switches at 1 for the internal nodes of the circuit (voltage Vcc), it will be understood that this consumption is not the same when R is equal to 1 and when R is equal to 0, including when the data applied at the inputs are identical.

The function selection signal R is refreshed (renewed at random) at precise instants to be

determined when the logic circuit is designed. If the sequence represented in Figures 6A, 6B is synchronized with a clock signal, signal R can be refreshed at each clock cycle or every K clock cycles, or even be
5 refreshed before the logic circuit 30 is used again (i.e., before each application of a new sequence of bits). When signal R is refreshed at random at each clock cycle or every K clock cycles, the timing diagrams showing the operation of circuit 30 comprise a
10 combination of the timing diagrams in Figure 6A and the timing diagrams in Figure 6B, according to the (random) value that signal R has at each clock cycle.

It will be understood that the method according to the present invention is susceptible to
15 any type of logic circuit embodiment. For that purpose, the topography of the logic circuit achieved by NAND gates (or NOR gates) only needs to be determined, then logic gates with two operating modes according to the present invention should be used
20 instead of the classical NAND gates. Inverting or non-inverting means according to the value of signal R, such as the EXCLUSIVE-OR gates described above, are then arranged at the inputs and outputs of the logic block thus achieved.

25 As it will be clear to those skilled in the art, the scrambling method according to the present invention is susceptible to various other embodiments. Although designing a logic circuit with two operating modes using elementary logic gates 10 with two inputs
30 was suggested above, logic gates according to the present invention with three or more inputs can be used. Furthermore, designing a logic circuit with two

operating modes can be done at the transistor level rather than at the gate level as described above.

This means that it is possible, by a determined transistor arrangement, to achieve a logic
5 circuit with two operating modes performing the same function regardless of the operating mode selected, while having different polarities on its internal nodes according to the operating mode selected. Equally, a logic circuit according to the present invention may
10 comprise different operating modes achieved by combining logic gates other than NAND or NOR gates, such as combinations of AND gates, OR gates, inverting gates, EXCLUSIVE-OR gates, for example.

Furthermore, although the logic circuit
15 described above performs the same function in two different ways, as part of the present invention, a logic circuit that performs the same function in three different ways, or four different ways, etc., can be provided. For that purpose, the following method may,
20 for example, be chosen.

The logic function to be performed is synthesized using a first type of logic gate to form a first logic block L1, and is then synthesized using a second type of logic gate to form a second logic block
25 L2, then using a third type of logic gate to form a third logic block F3, etc. Logic blocks L1, L2, L3... are then arranged in parallel. Their inputs are connected to a multiplexer and their outputs are connected to a demultiplexer. The multiplexer and the
30 demultiplexer are controlled by selection signal R (which, in this case, comprises several bits).

According to the value of signal R, the logic function is performed by one of the blocks L1, L2,

L3... This embodiment allows a DPA-type current monitoring attack to be countered, as each logic block has its own signature in terms of current consumption. In addition to this method of arranging logic blocks by
5 using conventional logic gates connected in parallel, a multifunctional logic circuit controlled by selection signal R can also be synthesized using multifunctional logic gates according to the present invention, so as to achieve interlaced logic functions that have common
10 internal nodes to counter probing attacks. A more in-depth integration can also be achieved by a design of the multifunctional logic circuit at the transistor level.

Figure 7 shows one application of the method
15 of the present invention to the embodiment of an encryption circuit CRYC that has a plurality of coding blocks CRY_0 to CRY_M . Each block is provided to receive data bits b_0 to b_N at an input and deliver a code bit, respectively C_0 to C_M . This encryption circuit
20 architecture is well known by those skilled in the art and corresponds, for example, to an encryption circuit of the 3DES type.

In accordance with the method of the present invention, each block CRY_0 - CRY_M is achieved using gates
25 with two operating modes according to the present invention (not shown). The data bits b_0 - b_N are applied to each block CRY_0 - CRY_M using individual EXCLUSIVE-OR gates controlled by the signal R, represented in a diagram by EXCLUSIVE-OR gates with N inputs receiving
30 bits b_0 - b_N and selection signal R. Similarly, each code bit C_0 to C_M is sampled at the output of each block

CRY₀-CRY_M using EXCLUSIVE-OR gates receiving the signal R at their other input.

Preferably, the signal R applied to each block CRY₀-CRY_M is statistically different from the signal R applied to the other blocks. Therefore, block CRY₀ and the EXCLUSIVE-OR gates associated to block CRY₀ receive a random bit R₀, block CRY₁ and the EXCLUSIVE-OR gates associated to block CRY₁ receive a random bit R₁..., and block CRY_M and the EXCLUSIVE-OR gates associated to block CRY_M receive a random bit R_M.

Figure 8 shows an example of the integration of the encryption circuit CRYC into a silicon chip forming a secured microprocessor MP. This silicon chip is designed to be mounted onto a portable support, such as a plastic card, for example, to form a smart card or any other equivalent portable electronic object.

The microprocessor MP comprises a central processing unit CPU, a memory MEM, the encryption circuit CRYC described above and registers PREG linked to input/output ports P₁, P₂,... P_n. These different components are connected to a data bus DTB. A random signal generator RGEN delivers function selection signals R₀ to R_M to each of the coding blocks of circuit CRYC (Fig. 7). The generator RGEN is activated by the unit CPU at each new session, i.e., after each microprocessor reset.

Thus, when a bit string is applied to the circuit CRYC at the start of the session to calculate an authentication code, the internal nodes of the coding blocks in the circuit CRYC have polarities and a current consumption that are not constant as compared

to the previous session, including when the bit string applied to the circuit CRYC is identical. The polarities of the coding block internal nodes vary from one session to the next according to a random law
5 specific to each block and independent of that of the other coding blocks.

The scrambling method according to the present invention is susceptible of being combined with other known scrambling methods, such as methods of
10 injecting noise into the supply circuit, and using a random internal clock signal, for example.